

ABSTRACT OF THE DISCLOSURE

Signcryption methods and apparatus are provided that combine the functions of signing and encrypting data to obtain private and authenticated communications. The signcryption methods are based on RSA and permit compact ciphertexts to be produced and non-repudiation to be provided in a straightforward manner.